SEMANTIC ANALYSIS ON COMMUNICATION AND SECURITY ISSUES OF EXTENSIBLE AUTHENTICATION PROTOCOL (EAP) ON WIRELESS Networks

[1]Dr.S.P. Anandaraj, [2]S. Poornima, [3]Sougandhika Reddy, [4]Sindhuja Manchala,
[5]Vedakshatha Puppala
[1]Associate Professor, [2]Assistant Professor, [345]UG Scholar, SR Engineering College, Warangal
Email: [1]anandsofttech@gmail.com, [2]Poornima.spa@gmail.com
,[3]Sougandhikareddyteena@gmail.com, [4]msindhu1121@gmail.com ,
[5]vedakshathamohan@gmail.com

ABSTRACT--Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become "wired", an increase in number of people need to understand the basics of security in a networked world. This network communication explains about the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the market place and understands risks and how to deal with them. Some history of networking is included, as well as introduction to TCP/IP (transfer control protocol & internet protocol) and inter networking. We go on to consider risk management, network threats, fire walls and more special purpose secure networking devices.The network communication reader will have a wider perspective on security in general, and better understand how to reduce and manage

Keywords: EAP Authentication Protocol, Security issues, Point to Point Protocol, Peer-to-Peer Networks

I. INTRODUCTION

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this paper, overview of some popular networks are discussed. In TCP/IP network protocol majorly suites the internet service providers and intranet service providers.

In Computer Networking, more no of threats occurs, it should be addressed by the network manager and administrators. This paper discusses on different type of threats and networks tools, that are used to reduce the exposure of risks of network computing. The Internet Engineering Task Force (IETF) has noticed the show progression in basic IEEE 802.11 standards as more security levels increased. Nowadays, almost all networks protocols adds more security features such as encrypted tunnels for exchanging various information (authentication, credentials and other data), dynamic key distribution and rotation, authenticating the user rather than the device, and applying identity-based mechanisms and systems. But, still there is need of more secured lightweight authentication is required, because more employed techniques slows down the system. Therefore, authentication protocol known as Extensible Authentication protocol (EAP) was introduced and it was versioned as many protocols, such as Protected EAP(PEAP), Lightweight Extensible Authentication Protocol

(LEAP) and EAP-Flexible Authentication via Secure Tunneling (EAP-FAST). The EAP was originally developed for Point to Point Protocol (PPP) and provides an infrastructure for network access clients and authentication servers.

II.EAP AUTHENTICATION PROTOCOL

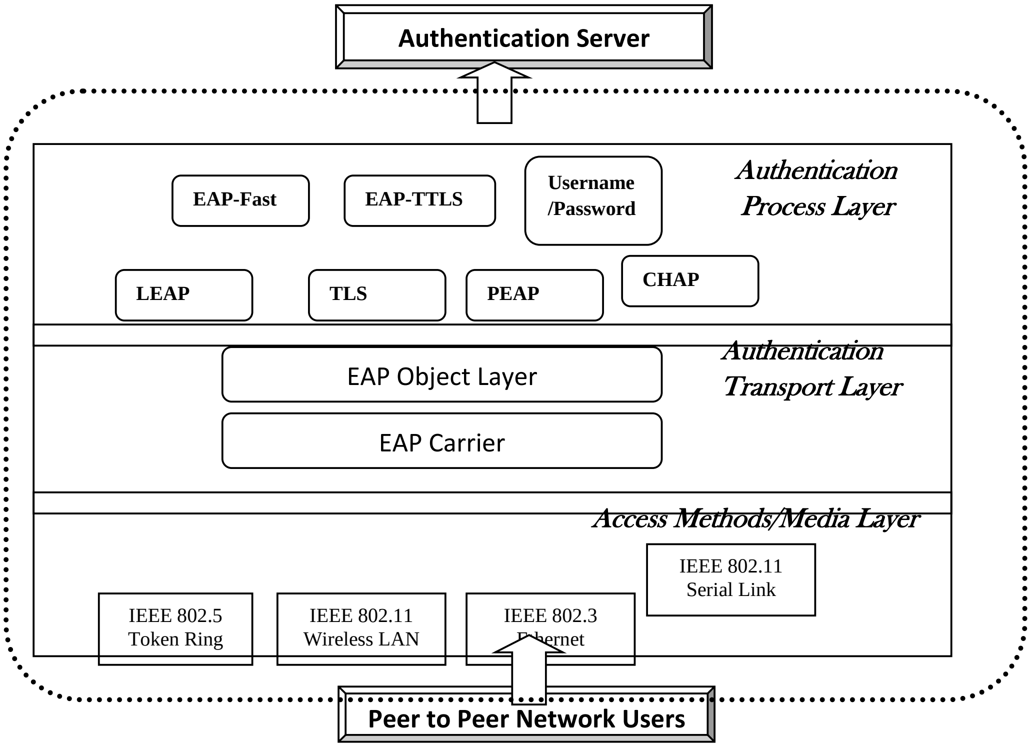
The EAP, a flexible protocol used to carry arbitrary authentication information, is defined in RFC 2284. (Incidentally, RFC 2284 is only 16 pages long!) A set of RFCs also defines the various authentication processes over EAP, including TLS, TTLS, SmartCard, and SIM. The IETF EAP workgroup is working on a revision of the EAP RFC and has submitted the new document as RFC 3579 (was RFC 2284bis).

EAP has two major features. First, it separates the message exchange from the process of authentication by providing an independent exchange layer. By doing so, it achieves the second characteristic: orthogonal extensibility, meaning that the authentication processes can extend the functionality by adopting a newer mechanism without necessarily effecting a corresponding change in the EAP layer.

III. LAYERED FRAMEWORK FOR EAP AUTHENTICATION

The above Figure.1 shows the authentication model is a layered one and has well-defined functionalities and protocols defining each layer and the interfaces between them. The access media can be any of the 802 media: Ethernet, Token Ring, WLAN, or the original media in the serial Point-to-Point Protocol (PPP) link. The EAP specifications provide a framework for exchanging authentication information after the link layer is established. The exchange does not even need IP. It is the function of the transport protocol layer (to specify how EAP messages can be exchanged over LAN, which is what 802.1x (and to some extent some parts of 802.11i) does. The actual authentication process is the one that defines how and what credentials should be exchanged. Bear in mind that this framework still does not say how the authorization should be done, such as what decisions are made and when. This functionality is completely left to the domain

Fig.1 EAP Layered Authentication Framework



IV. EAP IN COMMUNICATION

Figure.1 shows EAP communication with PPP, PPP peers do not choose a specific authentication mechanism during the link establishment phase of the PPP connection; instead, they negotiate to perform EAP during the connection authentication phase. Once the connection authentication phase is completed, the peers negotiate the use of a specific EAP authentication method. At this point, the conversation between the peers consists mostly of requests and responses for authentication information shown in figure.2. After that, EAP allows for an open-ended exchange of information between the access client and the authenticating server that varies depending on the connection parameters involved. In essence, the EAP method determines the length and details of the conversation between authenticating peers.

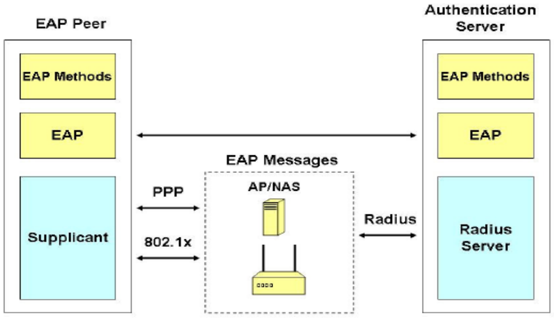


Fig.2 EAP Communication in PPP

The main components of EAP, as shown in Figure .2, are the following:

--*EAP peer/Access Clients*: Computers attempting to access network resources.

--*EAP authenticator*: An access point (AP) or network access server (NAS) requiring EAP authentication before granting access to a network resource.

--*Authentication server*: A server computer that negotiates the use of a specific EAP method with an EAP Access Client. It also validates EAP peers' credentials and authorizes access to network resources.

A supplicant is a software component that uses EAP to authenticate network access but that handles the actual data exchange [3]. In the example shown in Figure 2, both the EAP authenticator and the authentication server send EAP messages using RADIUS. As a result, EAP messages are actually exchanged between the EAP components on the EAP client and the authentication server. In a word, EAP provides the highest flexibility because it allows vendors to create more secure authentication schemes that can be plugged in later on, as required.

V. EAP IMPLEMENTATION

In wireless LANs, on one hand, Wi-Fi Protected Access (WPA) originally recommended EAPPSK—mainly, because home/small office applications were not required to support IEEE 802.1x authentication [4]. EAP-PSK is based on pre-shared keys—where a *shared secret key* is shared in advance between the two parties, using some secure channel [5]. EAP-PSK is a very lightweight protocol—it only requires four messages to complete the authentication stage [4]. Regardless of EAP-PSK simplicity and economy, WPA later recommended using EAP-TLS and EAPTTLS for increased security [4].

On the other hand, IEEE 802.11i (also known as WPA2) requires enterprise-level security. Therefore, in addition to EAP-TLS/TTLS, WPA2 devices also support PEAPv0, PEAPv1 and other open standards [4] [6].

Currently, the two most used EAP implementations are EAP-TTLS and PEAPv0. Both are extensively supported by most commonly used operating systems (Microsoft, Mac OS, and Linux) as well as by most network appliance vendors

A. EAP Frames

The 802.1x Extensible Authentication Protocol (EAP) also known as EAP over LANs (EAPOL) provides the framework for a device to authenticate when it connects to the network. When Port-Based Authentication is enabled, only EAPOL traffic is allowed on that port, everything else is dropped until the client is authenticated.

A client that connects to the network sends an EAPOL Start frame to initiate authentication, and the switch responds with an EAP Request/ID frame to request credentials. The client then sends an EAP Response/ID frame which contains credentials to the switch. The switch passes those credentials to the authentication server which then sends an EAP Request frame to the client to request a specific EAP Method for authentication. The client responds with an EAP Response frame. EAP Request frames and EAP Response frames are passed back and forth until the authentication server sends a EAP-Success message to the switch. At this point, the client is authenticated and normal traffic is allowed. When the client logs off, an EAPOL Logoff frame is sent to the switch and the port becomes unauthenticated.

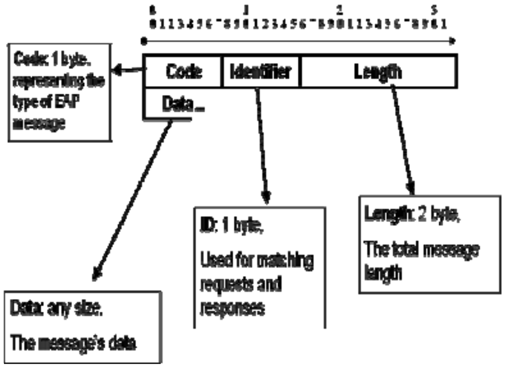

0 1 2 3
01234567890123456789012345678901
Code: 1 byte, representing the type of EAP message
Code
Identifier
Length
Data...
ID: 1 byte, Used for matching requests and responses
Length: 2 byte, The total message length
Data: any size. The message's data

Fig.3 EAP Frame Format

b. EAP Messages

The EAP message exchange is basic, as shown in Figure.3. EAP starts after the supplicant has data and link layer connectivity). The communication between the authenticator and the supplicant is done as a request-response paradigm, meaning a message is sent and the sender waits for a response before sending another message.

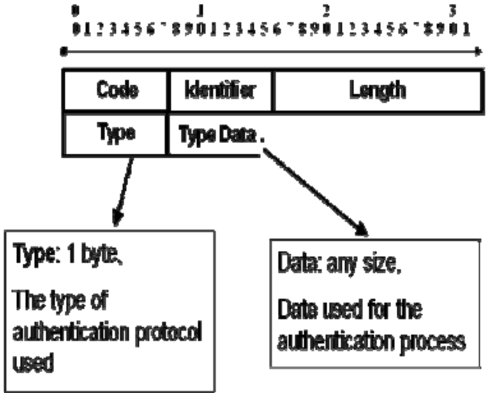

0 1 2 3
01234567890123456789012345678901
Code
Identifier
Length
Type
Type Data .
Type: 1 byte, The type of authentication protocol used
Data: any size, Data used for the authentication process

Fig.4 EAP Message Format

- EAP request and response messages have the same format , with code=1 for requests and code=2 for responses
- EAP Success messages are EAP messages with code 3 and no data.
- A success message means that the authentication concluded successfully.
- EAP failure messages are EAP messages with code 4 and no data.
- A Failure message means that the authentication has failed.

C. EAP Authentication Process

The Authenticator sends the peer an Identity request (optional).The Peer sends a response to the identity request identifying himself (optional).The Authenticator sends a request with a type according to which authentication method he wants to use and the data needed for the authentication. The Peer sends back a response of the same type or of type Nak signifying he refuses to use the requested authentication method. The Authenticator may at this point send another request (to repeat the process) or a success/failure message.If the authentication was successful and mutual authentication is required, the sides change roles and the authentication is repeated in the other direction.

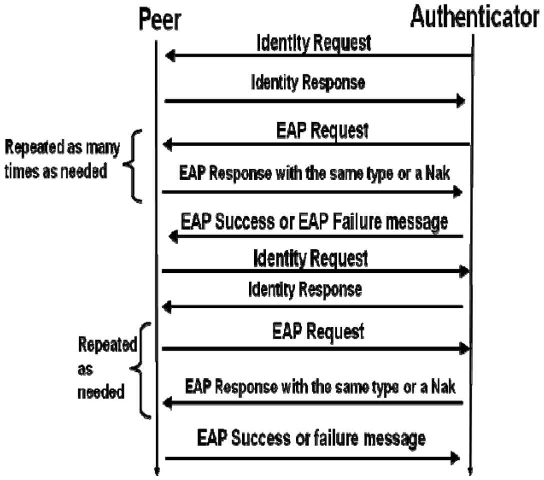

Peer
Authenticator
Identity Request
Identity Response
Repeated as many times as needed
EAP Request
EAP Response with the same type or a Nak
EAP Success or EAP Failure message
Identity Request
Identity Response
Repeated as needed
EAP Request
EAP Response with the same type or a Nak
EAP Success or failure message

Fig. 5 EAP Messages

VI.EAP SECURITY ISSUES

EAP is a standard that provides an infrastructure for network access clients and authentication servers. EAP does not specify the authentication mechanism itself but the way it is negotiated by the communicating parties. Consequently, EAP has no security issues in itself.

A. Dictionary Attacks

A dictionary attack is a technique for defeating a code or authentication mechanism by trying each word from a dictionary—a list of common words—and encoding it the same way the original passphrase was encoded [6] [7]. Dictionary attacks differ from brute-force attack on the fact that only the most likely words are tried

B. Plaintext Attacks

EAP implementations that rely on clear-text authentication using RADIUS (even within a protected tunnel) are vulnerable to known-plaintext attacks [2]. In a known-plaintext attack (KPA), the attacker uses samples of both the plaintext and its encrypted version to reveal further secret information such as the secret encryption key

C. Man-in-the-middle Attacks (MitM)

Tunneling protocols such as TLS and TTLS offer a server-authenticated tunnel that secures both the authentication method and the user's identity [12]. Unfortunately, original implementations of EAP that are based on these protocols may also be vulnerable to man-in-the-middle (MitM) attacks. In a MitM attack, a rogue client assumes the identities of both the client and the server in order to intercept communication from one device and send a tainted one to the other device

D. Ciphertext attacks

EAP-SIM improves the original GSM security model—based on a pre-shared key and challenge-response mechanism. The original GSM standard uses A5/1 and A5/2 stream ciphers with key length of 64 bits [13] [15]. EAP-SIM improves the original GSM standard by increasing the key length to 128 bits. Unfortunately, the way the new 128-bit key is generated has been shown to be defective [14]. Rather than being 128-bit long, the resulting key has an effective key length of 64 bits only.

VII. SEMANTIC ANALYSIS

To authenticate WLAN, IEEE 802.1x provides authentication framework based on Extensible Authentication Protocol(EAP). The EAP supports several authentication protocols and each protocol has advantages and disadvantages, respectively. It supports cellular-WLAN interworking and provides strong user identity protection. Moreover, our protocol has less overhead than other protocols(EAP-TTLS, PEAP, and EAP-UTLS) because of using a symmetric key cryptosystem and ECDH. Moreover, the protocol prevents man-in-the middle attack and replay attack. In addition, EAP protocol provides PFS and does not occur SQN synchronization which occurs in EAP-AKA. Therefore, our protocol provide more efficient and secure 3G-WLAN interworking than previous protocols.

VIII. CONCLUSION

Wireless communication having great features are attractive among users as well as service provides us. With the increase in its use security problems of confidentiality, integrity and authentication are also increasing. The mechanism to solve these problems has changed to public key cryptography from symmetric key cryptography. The available public key cryptographic approaches are good in security point of view but they are computationally extensive as well as have more signaling overhead. Furthermore, these approaches don't provide integrity of the initial authentication messages and authentication of the network.

As noted before, although, public key cryptography is computationally very extensive which requires large processing power, battery and memory, but still the approach we proposed is efficient to use than the others. The rapid developments in integrated circuits(IC) and smart cards(Example: SIM) technologies, high speed communication systems(Example:UMTS), and significance of secure transactions make the conditions more favorable to use public key cryptography.

EAP has been implemented based on several well-known authentication technologies. For instance there are versions of EAP built on top of PSK, TLS, TTLS, GSM, AKA, among many others. Unfortunately, some these implementations present significant security vulnerabilities such as exposure to dictionary attacks and man-in-the-middle attacks. To conclude, EAP is a highly flexible infrastructure for secure network access authentication. Thus far, it has been implemented in many flavors and colors, based on well-known authentication scheme, some of them with important security weaknesses.

References:

[1]. Snyder, EAP (Extensible Authentication Protocol): What is 802.1x? www.Networkworld.com., May 2002

[2]. IEEE Computer Society, IEEE Microwave Theory and Techniques Society, IEEE Standard for Local and Metropolitan Area Networks:Part 16. Air Interface for Fixed Broadband Wireless Access Systems,IEEE Std 802 16-2004. 1 October 2004.

[3]. Mandin, Enhancement of 802.16e to Support EAP-based Authentication/Key Distribution, 802.16e Security Ad Hoc Committee,http://www.ieee802 org/16/tge/contrib/C80216e-03_71r4.pdf

[4]. P. Funk, S. Blake-Wilson, EAP Tunneled TLS Authentication protocol version 1, February 2005.

[5]. Aboba, D. Simon, PPP EAP TLS Authentication Protocol, RFC 2716, October 1999.

[6]. D. Stanley, J. Walker, B. Aboba, EAP Method requirements for Wireless LANs, RFC 4017, March 2005.

[7]. L. Blunk, J. Vollbrecht, PPP Extensible Authentication Protocol (EAP), RFC 2284, March 1998.

[8]. B. Aboba, L. Blunk, J. Vollbrecht, J.Carlson, and H. Levkowetz. Extensible authentication protocol (EAP). The Internet Engineering Task Force - Request for Comments: 3748, June 2004.

[9]. Ma, Y. and Cao, X. (2003) 'How to use EAP-TLS Authentication in PWLAN Environment', IEEE,Paper presented at the 2003 International conference on neural networks and signal processing, 14–17 Dec, Vol. 2, pp.1677–1680. In proceedings.

[10]. Shumman, W. and Ran, T. (2003) 'WLAN and it's Security problems', IEEE, Paper presented at the 2003 International conference on Parallel and Distributed Computing, Applications and Technologies, pp.241–245. In proceedings.

[11]. Donald J.Welch and Scott D. Lathrop. A Survey of 802.11a Wireless Security Threats and Security Mechanisms. Technical Report ITOC-TR-2003-101,United States Military Academy, 2003.